UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,415	11/14/2003	Sherman (Xuemin) Chen	15225US01	2739

23446 7590 03/06/2007

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,415	CHEN ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☒ Claim(s) *3-5,13-15 and 23-25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/2/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 11/14/2003.

Claim Objection

2. Claims 3 – 5, 13 – 15 and 23 – 25 are objected because the claim language "equivalent to" is considered to be ambiguous in its meaning and its context about what exactly to constitute the degree of equivalence and as such appropriate corrections are required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 2, 6, 10 – 12, 16, 20 – 22, 26, and 30 – 31 are rejected under 35 U.S.C. 102(e) as being anticipated by Sprunk et al. (U.S. Patent 2003/0007644).

As per claim 1, Sprunk teaches a method for producing a secure key, the method comprising:

receiving at least a first input key, a second input key and a third input key (Sprunk: Figure 4 and Para [0036]: Key-1, Key-2 are qualified as a first input key, a second input key, respectitively and the IV (Initial Value) is considered as one of key variation values and is qualified as a third input key); and

generating a first output key based on said at least said first input key, said second input key and said third input key (Sprunk: Figure 4 and Para [0036]), wherein said first output key is unique and differs from said at least said first input key (Sprunk: Figure 4, Para [0017] Line 4 – 5 and Para [0036] Line 12: (a) the IV, Key 1 and Key 2 are known and DES generator 420 to generate a key that is used, in turn, by DES generator 425 to generate another key (Para [0036] Line 12) – i.e. the stage of dual DES generator generates a different / another key from the input key-1 and input key-2; Examiner notes another key, as per its context value or the stored location of the key, can be broadly interpreted as a different key to meet the claim language and (b) Sprunk teaches the desirable output key should not be repeated (Para [0017] Line 4 – 5).

As per claim 11 and 21, Sprunk teaches a machine-readable storage having stored thereon, a computer program having at least one code section for producing a secure key, the at least one code section being executable by a machine for causing the machine to perform steps (Sprunk: Figure 1 & 4 and Para [0028]) comprising:

receiving at least a first input key, a second input key and a third input key (Sprunk: Figure 4 and Para [0036]: Key-1, Key-2 are qualified as a first input key, a second input key, respectitively and the IV (Initial Value) is considered as one of key variation values and is qualified as a third input key); and

generating a first output key based on said at least said first input key, said second input key and said third input key (Sprunk: Figure 4 and Para [0036]), wherein said first output key is unique and differs from said at least said first input key (Sprunk: Figure 4, Para [0017] Line 4 – 5 and Para [0036] Line 12: (a) the IV, Key 1 and Key 2 are known and DES generator 420 to generate a key that is used, in turn, by DES generator 425 to generate another key (Para [0036] Line 12) – i.e. the stage of dual DES generator generates a different / another key from the input key-1 and input key-2; Examiner notes another key, as per its context value or the stored location of the key, can be broadly interpreted as a different key to meet the claim language and (b) Sprunk teaches the desirable output key should not be repeated (Para [0017] Line 4 – 5).

As per claim 31, Sprunk teaches a system for producing a secure key, the system comprising:

a mapper (Sprunk: Figure 4 / Element 420 / 425 and Para [0036]: the first stage of dual DES Key Generator is considered as a key mapper);

a scrambler coupled to said mapper (Sprunk: Figure 4 / Element 450 / 455 / 456 and Para [0039]: the second stage of dual DES key scrambler (i.e. the key hashing function) can be considered as the scrambling function);

a masker coupled to said mapper (Sprunk: Figure 4 / Element 435 / 437 and Para [0036]: the AND gate is considered as a masking function);

a key generator coupled to said scrambler mapper (Sprunk: Figure 4 / Element 465 / 470 and Para [0039]); and

an XOR operator coupled to said masker and said scrambler (Sprunk: Figure 4 / Element 460 and Para [0039]: the Adder (i.e. an equivalent XOR entity (Figure 4 / Element 460)) performs an exclusive ORing function).

As per claim 2, 12 and 22, Sprunk teaches said first input key is a customer key, said second input key is a customer key selection and said third input key is a key variation (Sprunk: Para [0036] and Para [0037]: The IV, Key 1 and Key 2 are known and supplied, for example, by a governmental agency – the customer is government agency and the IV is consider as a key variation).

As per claim 6, 16 and 26, Sprunk teaches mapping said at least said first input key, said second input key and said third input key to generate mapped output key data (Sprunk: Figure 4 / Element 420 / 425 / 427 and Para [0036]: the output key data from the first stage of dual DES key generator at Figure 4 / Element 427 is considered as mapped output key data to meet the claim language).

As per claim 10, 20 and 30, Sprunk teaches transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt

information (Sprunk: Figure 3 / Element 340 and Para [0035] Line 9 – 11: the new output key is used to encrypt the information).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 3 – 5, 13 – 15 and 23 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprunk et al. (U.S. Patent 2003/0007644), in view of Schneier ("Applied Cryptography, Second Edition", 1996).

As per claim 3, 13 and 23, Sprunk teaches the desirable output key should be unique (Sprunk: Para [0017] Line 4 – 5: the output key should not be repeated). However, Sprunk does not disclose expressly the desirable output key is not equivalent to said at least said first input key.

Schneier teaches the desirable output keys is not equivalent to said at least said first input key (Schneier: Page 282, 2nd Para / Line 3: a complementary key is interpreted as an equivalent key and should be tested and avoided).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Naclerio within the system of Sprunk because (a) Sprunk teaches a method for generating, from the input keys, an encryption output key that should not be weaken for the purpose against hostile attackers (Sprunk: Para [0041] and [0007]) and (b) Schneier teaches a complementary key is interpreted as an equivalent key and should be tested and avoided in that situation (Schneier: Page 282, 2nd Para / Line 3).

According Sprunk in view of Schneier teaches:

determining whether said first output key is at least one of a unique key and is not equivalent to said at least said first input key (Sprunk: Para [0017] Line 4 – 5 & Para [0036] & Schneier: Page 282, 2nd Para / Line 3: (a) Sprunk teaches the desirable output key should be unique (Para [0017] Line 4 – 5: the output key should not be repeated (b) Schneier teaches the users should be warned unless the output key is not a complement key – i.e. a complementary key is interpreted as an equivalent key and should be tested and avoided).

if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key, generating a second output key based on a modified one of at least one of said first input key, said second input key and said third input key (Sprunk: Figure 4, Para [0037] – [0039] and Para [0041]: Examiner notes the prior-art teaches generating a second output key (Figure 4 / Element 465) from the first output key (Figure 4 / Element 427) regardless the outcomes of the IF condition that can meet the claim limitation since the IF-NOT (i.e. ELSE) condition is not recited in the claim and

the prior-art evidently always covers the IF condition by generating a second output key regardless – i.e. the original contribution from the first input key, second input key or third input key is modified by (a) using a feedback loop to replace the IV value via a switch (Figure 4 / Element 417), and (b) the key space size variable (Figure 4 / Element 430) is also used as a key variation for modification purpose and the subsequent one-way key hashing function (Figure 4 / Element 456) is further employed to generate a second output key to avoid a weaken output key).

As per claim 4, 14 and 24, Sprunk as modified teaches determining whether said second output key is at least one of a unique key and is not equivalent to said at least said modified one of at least one of said first input key, said second input key and said third input key (Sprunk: Para [0017] Line 4 – 5 and Para [0036] & Schneier: Page 282, 2nd Para / Line 3: (a) Sprunk teaches the desirable output key should be unique (Para [0017] Line 4 – 5: the output key should not be repeated (b) Schneier teaches the users should be warned unless the output key is not a complement key – i.e. a complementary key is interpreted as an equivalent key and should be tested and avoided).

As per claim 5, 15 and 25, Sprunk as modified teaches said first output key and said second output key are not weak or semi-weak keys (Sprunk: Figure 4, Para [0037] – [0039], Para [0041], Para [0029] Line 1 – 4 and Para [0007]: the selection and distribution may also be non-random and therefore, the output key has the key-bit

randomly distributed over a key space corresponding to B-bit keys again from N-bits (Para [0037] – [0039] and Para [0041]), which is thereby not weaken for the purpose against hostile attackers (Para [0007] Line 13 – 15)).

5. Claims 7 – 9, 17 – 19 and 27 – 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprunk et al. (U.S. Patent 2003/0007644), in view of Bennett et al. (U.S. Patent 4,864,615).

As per claim 7, 17 and 27, Sprunk teaches an intermediate key of Key-3 or Key-4 (Figure 4 / Element 440 / 445) for DES key generator. However, Sprunk does not disclose expressly generating an intermediate key based on said first input key.

Bennett teaches generating an intermediate key based on said first input key (Bennett: Column 6 Line 65 – 67 / Line 59 – 62 and Figure 2 / Element 18 & 42: a first intermediate key is generated based on the first-key (pre-key) associated with a DES key encryptor).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bennett within the system of Sprunk because (a) Sprunk teaches a method to provide cryptographic keys for DES cryptographically processing information systems (Sprunk: Abstract / Line 1 – 2 and Para [0003]) and (b) Bennett teaches a key security system for reproducing DES secure keys by using distributed key generation data and a distributed encrypted pre-key with a

secured chain of protection for generated keys (Bennett: Column 2 Line 18 – 21, Column 3 Line 43 – 46 Column 6 Line 65 – 67 / Line 59 – 62).

As per claim 8, 18 and 28, Sprunk as modified teaches scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output (Sprunk: Figure 4 / Element 450 / 455 / 456 and Para [0039]: the second stage of dual DES key scrambler (Figure 4 / Element 450 / 455) is qualified as a scrambler with two input data: (a) a generated intermediate key of Key-3 or Key-4 from the first key and (b) the output data of AND gate at Figure 4 / Element 437 sourced from the generated mapped output key data).

As per claim 9, 19 and 29, Sprunk teaches masking at least a portion of said generated mapped output key data (Sprunk: Figure 4 / Element 435 / 437 and Para [0036]: the AND gate is considered as a masking function); and exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key (Sprunk: Figure 4 / Element 460 and Para [0039]: the adder (i.e. XOR entity of Figure 4 / Element 460) performs an exclusive ORing function on the scrambled output at Figure 4 / Element 456 derived from the second stage of dual DES key scrambler and the output data of AND gate at Figure 4 / Element 437 sourced from the generated mapped output key data).

6. Claims 32 – 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprunk et al. (U.S. Patent 2003/0007644), in view of Naclerio (U.S. Patent 7,028,014).

As per claim 32, Sprunk teaches a key output of XOR operator (Sprunk: Figure 4 / Element 460 and Para [0039]: the adder (i.e. XOR entity (Figure 4 / Element 460)) performs an exclusive ORing function) and transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information (Sprunk: Figure 3 / Element 340 and Para [0035] Line 9 – 11: the new output key is used to encrypt the information).

However, Sprunk does not disclose expressly at least one processor coupled to an output of said XOR operator.

Naclerio teaches at least one processor coupled to an output of said XOR operator (Naclerio: Column 4 Line 1 – 9: encrypting the data and storing it again in the memory – this encryption is performed by the processor executing encryption software in the memory (ROM) or optionally be performed by an encryption engine).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Naclerio within the system of Sprunk because (a) Sprunk teaches transferring the output key to an encryptor for encrypting information (Sprunk: Figure 3 / Element 340 and Para [0035] Line 9 – 11) and (b) Naclerio teaches a typical structure of an encryptor that can perform encryption functions (Naclerio: Column 4 Line 1 – 9).

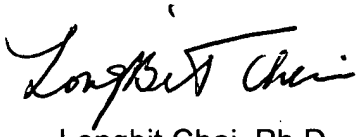
As per claim 33, Sprunk as modified teaches an encryption engine that is coupled to an output of said XOR operation (Sprunk: Figure 4 / Element 460 and Para [0039]: the adder (i.e. XOR entity (Figure 4 / Element 460)) performs an exclusive ORing function) and transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information (Sprunk: Figure 3 / Element 340 and Para [0035] Line 9 – 11: the new output key is used to encrypt the information).

As per claim 34, Sprunk as modified teaches a memory coupled to at least one of said encryption engine and said at least one processor (Naclerio: Column 4 Line 1 – 9: encrypting the data and storing it again in the memory – this encryption is performed by the processor executing encryption software in the memory (ROM) or optionally be performed by an encryption engine).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
2/25/2007